学校编码：10384
学号：19020101152508
分类号_____密级_____
UDC_____

厦门大学

硕 士 学 位 论 文

标准模型下基于身份的入侵容忍签名

ID-based Intrusion Resilient Signature without Random Oracles

蔡 建 霞

指导教师姓名： 曾 吉 文 教授
专 业 名 称： 基础数学
论文提交日期： 2013 年 月
论文答辩时间： 2013 年 月
学位授予日期： 2013 年 月

答辩委员会主席：_____
评 阅 人：_____

2013 年 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

在密码和信息安全领域, 密钥的安全性是一个非常重要的问题. 密钥安全相关密码体系应运而生. 秘密共享、门限密码、前向安全密码、密钥隔离密码、入侵容忍密码、安全的密钥提取协议都是密钥安全十分重要的部分. 最早的入侵容忍方案是 2002年 Itkis和 Reyzin提出的签名者基础的入侵容忍签名方案, 其中结合了前向安全性、密钥隔离及动态安全的优点. 此后, 入侵容忍签名快速发展, 安全性及效率得到很大提高. 并在基于身份的签名方案中得到应用. 2012年, 于佳等人在前向安全签名方案和入侵容忍方案的基础上, 提出了基于身份随机喻示模型下的入侵容忍签名方案, 并在CDH假设下可证明安全.

本文提出了一个标准模型下可证安全的, 基于身份的入侵容忍签名方案. 此方案与传统签名方案相比有明显优势. 传统签名方案的安全性依赖于密钥的保密性, 一旦密钥泄露, 用该密钥得到签名都需要重新定义. 入侵容忍签名很好地解决了这一问题. 无论敌手入侵基地和用户多少次, 除入侵时间段外的签名都是安全的. 即使同时入侵, 获得所有秘密信息, 仍不可伪造以前时间段的签名. 本文方案具有良好的性能, 所有时间参数及存储空间大小的复杂度都不会超过 $O(logT)$. 并证明, 若 CDH假设是困难的, 则方案在标准模型下是安全的.

关键词： 入侵容忍安全; 基于身份的签名; 标准模型.

Abstract

The security of secret key is a very important problem in the field of cryptology and information security. Cryptosystem related to secret key security emerges. Secret sharing, threshold cryptography, forward secure cryptography, key-insulated cryptography, intrusion-resilient cryptography, secure key retrieval protocol are important parts of work related to secret key security. The earliest intrusion-resilient system was proposed by Itkis and Reyzin in 2002. It is an intrusion-resilient signature with the advantages of forward secure cryptography, key-insulated cryptography and dynamic security. Subsequently, intrusion-resilient signature has been fully developed, with considerable improvement of security and efficiency. It has been used in ID-based signature. In 2012, Yu Jia et al proposes an ID-based intrusion resilient signature with random oracles which is provably secure under CDH assume based on forward secure cryptography and intrusion-resilient cryptography.

An ID-based intrusion resilient signature without random oracles is present in this paper. This scheme is far superior to traditional schemes. Traditional ID-based signatures' security depends on the assumption that the secret keys are secure. Once the key is exposed, the signatures associated with this key have to be reissued. Intrusion resilient signature totally solves this problem. No matter how many times the scheme is intruded, signatures in any other time is secure, as long as the enemy doesn't compromise the base and the signer at the same time. Otherwise, the signatures before the intrusion time can't be forged. The scheme in this paper has nice property, all the parameter and storage space is no bigger than $O(logT)$. And in the end, if CDH problem is hard, our scheme is provably secure in standard model.

Key Words: intrusion-resilient security; ID-based signature; without random oracles.

目 录

CONTENTS

第一章　绪 论

1.1 研究背景

随着计算机软硬件及网络技术的飞速发展, 各种网络服务已经渗透到人们生产生活的各个领域. 这的确给人们的活动带来了巨大的便利和好处, 同时却也带来了前所未有的威胁. 网络攻击、网络病毒在不断地变种、升级, 严重威胁企业及个人信息安全. 网络信息安全正随着全球信息化步伐的加快而显得日趋重要. 信息安全即指信息的完整性、可用性、保密性和可靠性. 密码及信息技术能有效解决这一问题.

在密码和信息安全领域中, 密钥的安全性是一个非常重要的核心问题. 一旦密钥泄露了, 无论密码算法多么强大, 对应于这个密钥的所有操作都是不安全的. 密钥泄露, 系统将不得不更换新的公钥和私钥, 否定所有以前的工作. 对于基于身份的密码系统尤甚, 这是因为用户身份是不容易改变的. 因此密钥泄露严重威胁着密码体系的安全, 如何利用密码学的方法来减小密钥泄露的可能性, 以及在密钥泄漏时, 如何减低其对系统造成的伤害, 是十分有意义的研究工作.

1.1.1 基于身份的密码体制

在公钥密码体制中, 密钥都是成对出现的，每一对密钥由一个公钥和一个私钥组成. 私钥由拥有者自己保存, 而公钥要公之于众. 为了公钥体系的广泛应用, 一个基础性的问题就是公钥的分发和管理. 公钥本身没有标记, 仅从公钥本身无法判断用户的身份. 因此, 公钥密码体制使用公钥证书的方法在公钥和用户身份间建立联系. 但在对证书的管理和支持及结构上的配置是传统公钥密码体制比较复杂的问题之一.

1984年, Shamir在[1]中第一次提出了基于身份的密码体制, 并给出了一个基于身份的数字签名方案 (IBS). 在[1]系统中不需要证书, 可以使用用户自身的物理标识如姓名、 IP地址、电子邮箱地址等做公钥. 用户的私钥由一个被称为私钥生产器 PKG的可信任第三方计算得到. 然而, 直到 2001年, Shamir意义上的基于身份的加密方案 (IBE)才真正被提出[2]. 这要归功于 Boneh和 Franklin. 该方案利用椭圆曲线的双线性对进行构造, 在随机预言模型下的安全. 2003年, Canetti等人提出了一种标准模型下的 IBE方案[3], 但该方案需要对身份的每一比特计算双

线性映射, 计算量大, 不适合实际应用. Boheh和 Franklin在 2004年提出来三个在标准模型下安全的 IBE方案, 分别在文献[4][5]中. 2005年, Water在[5]的基础上提出来一个更加有效的标准模型下安全的 IBE 方案[6]. 目前, 基于身份的方案包括基于身份的加密体制、签名体制、可鉴别身份的加密和签密体制、密钥协商体制、门限密码体制、前向安全密码体制、强前向安全密码体制等.

1.1.2 入侵容忍安全

为减小密钥泄露的对基于身份签名的危害, 一个有效的方法就是赋予数字签名前向安全性的特征. 最早由 Anderson在[7]中提出. Canetti等人提出了第一个基于双线性对的前向安全公钥加密方案, 并使用了二进制树加密的方法[8]. 此后, [9][10][11]受此启发, 提出了性能更好的基于双线性对的前向安全签名方案. 在前向安全签名方案中, 把整个签名的生命周期划分为 T个离散的时间段, 在每个时间段结束时, 利用单向函数更新密钥. 公钥在整个生命周期中保持不变. 因此, 在当前密钥泄露时间段前的签名是安全的, 不可伪造的. 然而, 此方案并无法保证密钥泄露已后时间段签名的安全. 为解决这一问题, 密钥隔离方案在[12]被 Dodis等人提出. 在这一系统中, 有两个实体, 一个签名用户, 一个基地. 签名用户利用私钥进行签名. 在每个时间段结束时, 签名用户将联合基地进行密钥演化得到下一时间段密钥. 因此, 假若基地是安全的, 即使入侵者得到当前签名密钥, 没有基地的帮助也无法计算密钥泄露时间段以后的签名密钥, 文献[13][14]对此进行进一步了研究.

下面主要介绍入侵容忍安全.

最早的入侵容忍签名方案是 2002年, Itkis和 Reyzin在[15]中提出签名者基础的入侵容忍签名方案, 其中结合了前向安全性、密钥隔离及动态安全的优点, 安全性依赖于强 RSA假设, 但其密钥产生和演化效率较低. 在入侵容忍签名中, 与密钥隔离签名一样, 有两个实体, 一个签名用户, 一个是基地, 签名由签名用户独立完成, 基密钥仅用于密钥的演化与更新. 用户和基地在每个时间段都会有任意多次更新密钥的操作, 这使得即使敌手入侵用户基地任意多次, 只要敌手不同时入侵, 就无法计算其他时间段的签名. 即使同时入侵, 也无法获得以前时间段的签名. 因此, 无需保证基地是安全的. 其后的2003年, Itkis提出了标准模型下 g-入侵容忍签名[16]. 同年, 在[17]中 Dodis等人提出了公钥入侵容忍加密的概念并给出了一个较有效的密钥更新方式, 这对入侵容忍签名的发展也是有相当的意义. 2006年, Libert[18] 提出了在标准模型下的有效的入侵容忍签名, 这使入侵容忍签